THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 17, Number 2/2016, pp. 186–192

EXTENSION OF CYSEMOL FOR CLOUD COMPUTING INFORMATION SECURITY ASSESSMENT

Justinas JANULEVIČIUS, Antanas ČENYS, Nikolaj GORANIN

Vilnius Gediminas Technical University, Dept. of Information Systems. Sauletekio al. 11, LT-10223, Vilnius, Lithuania
Corresponding author: Justinas JANULEVIČIUS, E-mail: justinas.janulevicius@vgtu.lt

Abstract. The emerging cloud computing paradigm enables countless possibilities for cost saving, rapid growing architectures with a pay-as-you-go model. However, it also brings drawbacks typical for any emerging technology – immaturity of security management is one of them. Automated information security assessment systems – a relatively new subject on its' own – offers solutions for ensuring security and modeling of security breaches as a preventive action. This paper presents an approach to cloud security evaluation model that is later implemented to an advanced enterprise architecture analysis system – Cyber Security Modeling Language (CySeMoL) for automatic multi-perspective cloud security information risk assessment.

***Key words**:* Cyber Security Modeling Language, Cloud Computing, Enterprise Architecture, Security Assessment.

1. INTRODUCTION

Cloud computing is one of the most promising modern technologies in the field of Information Technology (IT), bringing many benefits and enabling earlier unavailable IT solutions. However, there are security issues, and due to the immaturity of the technology, there is great room for ambiguity when it comes to dealing with them. Cloud can be a much safer environment compared to any data-center, given a proper security architecture is deployed. This is especially applicable to non-security-competent enterprises. However, lack of skills and knowledge of the cloud security requirements might run the whole enterprise down [1].

Using Enterprise Architecture Security Assessment Tools, such as Cyber Security Modeling Language (CySeMoL) for implementation of information security related models provides the end user with improved accessibility and the ability to assess critical areas of the design prior to its' deployment, preventing possible damages. Therefore, implementation of cloud security assessment model comes as a natural solution to this problem. Moreover, since CySeMoL already covers a broad range of domains of enterprise architecture, cloud security assessment enables users of the system to cover their complete IT infrastructure that, in case of an enterprise, is a combination of diverse technology [2].

This paper presents an approach to cloud security evaluation model that is implemented to Cyber Security Modeling Language (CySeMoL) for automatic multi-perspective cloud security information risk assessment. It gives a clear understanding of cloud security aspects for the enterprise as well as enables the designer to perform deep security analysis prior to the deployment of the cloud.

2. RELATED WORKS

Modeling languages such as SySML [3], Business Process Modeling Notation (BPMN) [4] enable creation of information system architecture and system environment through diagrams that can be used for various forms of analysis, one of which is security. Some of them offer extensions for Industrial Control System Security Analysis [5], and on top layer, Cloud Security [6]. The decision makers of the enterprise require solutions for cyber security estimation that are easy to understand [7]. There are various tools available for this purpose including CORAS and its' extension for ISO standard compliance [8], MulVAL [9] or NetSPA [10].

There are, however, only a few solutions that offer modeling capabilities along with the reasoning based on the systemized expert knowledge base. One of them is OpenMADS [11], the other is Cyber Security Modeling Language (CySeMoL) [2]. This research is based on the latter due to the better readiness and more complete database as well as lack of proper documentation for the OpenMADS. It does not offer modeling of enterprise architecture, rather supports state machine modeling which limits it to availability aspects only.

Cloud computing security covers topics, ranging from hardware and platform technologies to regulatory compliance and the effect of the variety of endpoint devices [12].

3. INFORMATION SECURITY MODELING

Enterprise architecture of information systems is a complex structure, built of components provided by different manufacturers using different architectures. Legacy systems come as an issue as well [13]. Cyber Security Modeling Language (abbreviated as CySeMoL) offers an expert knowledge meta-model based realization of an automated estimation of cyber security of enterprise architectures. The realization works as an attack-graph tool, where the accuracy of estimation depends on the granularity of the analyzed extendable model [7].

3.1. Analysis of Cloud Computing Security Vectors

Technical reports on cloud computing security assessment [14] deal with technical documentation, issued by trusted sources. One of which, the ENISA report on Cloud Computing [15] provides a number of vulnerabilities, covering domain. This paper uses the technical vulnerabilities, and especially the ones that are typically exposed to malicious activities rather than the ones that occur due to environmental circumstances. A collection of the aforementioned vulnerabilities is presented and commented in Table 1. This table is used as a reference to find the missing concepts in CySeMoL in the field of cloud computing.

Table 1

Mapping of technical vulnerabilities of cloud computing with CySeMoL concepts

Vulnerability	Comment	Related CySeMoL Concept
V1. AAA vulnerabilities V2. User provisioning V3. User de-provisioning	Clouds exposed to public networks require effective AAA controls.	PasswordAuthenticationMechanism, PasswordAccount
V4. Remote access to management interface	Allows end-point client vulnerabilities to compromise the cloud infrastructure	ApplicationServer, WebApplication
V5. Hypervisor vulnerabilities	Controls physical resources as well as virtual appliances on top of it. Solution suggested in [16].	OperatingSystem, SoftwareProduct
V6. Lack of resource isolation V17. Possibility that internal network probing will occur V18. Possibility that co-residence checks will be performed	Multi-tenancy caused information leakage using side-channel attacks. Solution suggested in [17]. Can lead to compromising of shared hard disk and memory as well as database. Moreover can have impact on parallel hypervisor on the cloud [14].	NetworkZone, ZoneManagementProcess, Firewall, IPS
V8. Communication encryption vulnerabilities V9. Lack of or weak encryption of archives and data in transit V10. Impossibility of processing data in encrypted form V11. Poor key management procedures	Communication encryption shortcomings enable malicious activities, such as eavesdropping. Discussed and sorted out in [18].	Protocol, Dataflow, NetworkInterface
V16. No control on vulnerability assessment process	Port scanning, vulnerability testing.	NetworkVulnerabilityScanner, IPS, IDSSensor

3.2. Cloud Computing Security Attack Surface

To assess the security of an architecture, scenarios, called the attack vectors, of how malicious activity may be executed have to be defined. The aggregation of these vectors provides a complete picture of probable attacks. It is defined as the attack surface [19].

Cloud computing security attack surface is a broader subject compared to the conventional client-server model due to the need of communicating over public networks that are by nature less secure than internal networks. Moreover, when using the public cloud model, the same infrastructure is shared among multiple users (or tenants) leaving a possibility of side-channel attacks in shared resources.

Based on the model by Gruschka and Jensen [20] cloud computing scenario is modeled based on three classes of participants: users, services and providers. In this model, every cloud computing scenario interaction can be addressed to two entities. Therefore, every attack vector here is detailed as a set of three-class bi-directional model interactions. Based on this concept, the reasoning, designed for client-server type of services only covers one out of three edges of the model, therefore only two surfaces.

When dealing with public cloud service providers, most of the security aspects inside the cloud architecture are managed by the provider, so the usage of the outsourced infrastructure is based on trust. Level of trust and responsibility from technical aspects is managed setting up a contractual relationship between the customer and the provider. It is typically achieved by applying the service level agreement (SLA) upon the subject. An international standard covering this domain [21] is being prepared, although guidelines for cloud service level agreement standardization [22] have already been published and fully cover the SLA aspect of cloud computing security. Based on the resource management architecture provided in [23], it is an essential component that must be taken into account.

3.3. Development of Information Security Model Extension for Cloud Computing

To enable the cloud computing information security assessment in CySeMoL there is a need to find the areas already covered by it as well as the missing components. Comparing security documentation to the classes provided by the CySeMoL defines the missing components and the solutions needed to cover them.

3.4. Coverage of Contractual Agreements

As introduced in Chapter 4.3, there is a need to integrate the measures of contractual agreements to CySeMoL in order to define the responsibilities of the security issues for the customer as well as vendor. The Service Level Agreement is the cornerstone of contractual agreements [24] that provides fundamental grounds for [22]:

- Quality of Service (QoS) – ensuring that the infrastructure would ensure proper quality of service;
- Quality of Protection (QoP) – that denotes the means to ensure the information security;

3.5. Implementation of Research Data to Cyber Security Modeling Language

The meta-concepts of the CySeMoL model are represented as classes with two types of attributes – `defense` and `attack step`. The model contains constrains for allowed object pairing, and the possible relations between them, so various types of relations can be granted for the same architecture depending on the situation. The assessment process is achieved by setting up an `Attacker` object that, depending on the objects it is connected to, may have different target goals. The attacker can have connections to multiple objects, thus enabling a much more complicated multi-perspective information security assessment [7].

Based on [22], the objectives dealing the security of the cloud from the SLA point of view are presented in Fig. 1. Considering that these objectives represent security issues, they can be mapped to the `defense` category attributes of the new SLA class. This class falls to the preventive class category, therefore it should not connected sequentially to the whole network path.

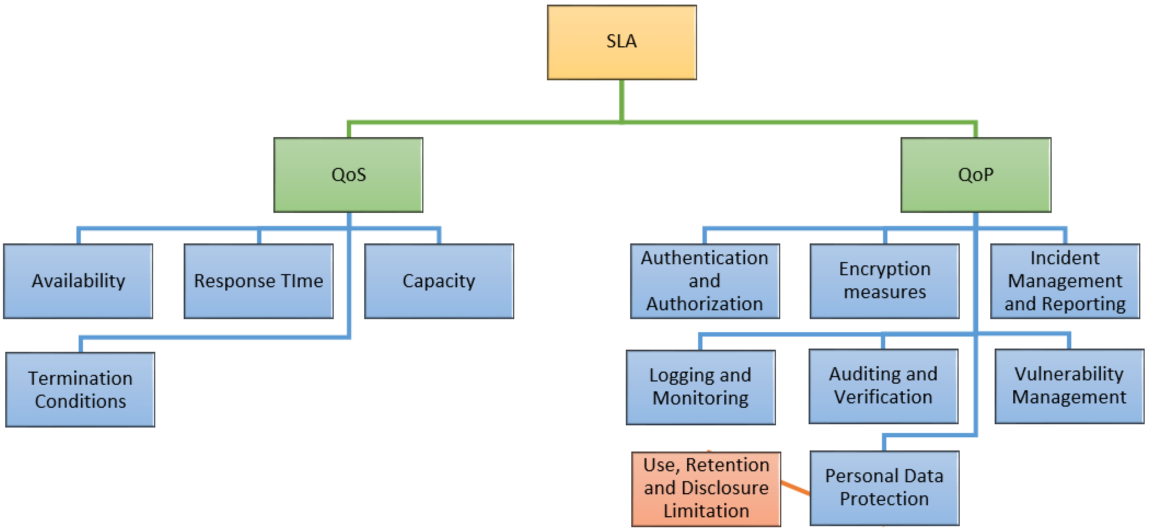

Fig. 1 – The Service Level Objectives for the SLA Concept [22].

3.6. Proposed Integration of Cloud Specific Technical Components

The model represents a simplified version of a cloud infrastructure security assessment model for the CySeMoL language based on [25]. It is structured referring to [7] as follows: `SoftwareProduct` in this case is a primary version of a hypervisor with no patches or updates. It has an instance in `OperatingSystem` which has the patching issues sorted. Moving along there is `ApplicationServer` that is connected to the `OperatingSystem`, which means that the server operates the machine, while `ApplicationServer` connection to `SoftwareProduct` denotes of what type of server is concerned. Connecting the following object – `WebApplication` to `ApplicationServer` states that this server acts as a web server. Adding a `Datastore` object defines the ability of the server to store data. The server has a connection to a `NetworkZone`, which means that it is possible to interface by the systems on the network [7]. The graphical representation of this model is provided in Fig. 2.

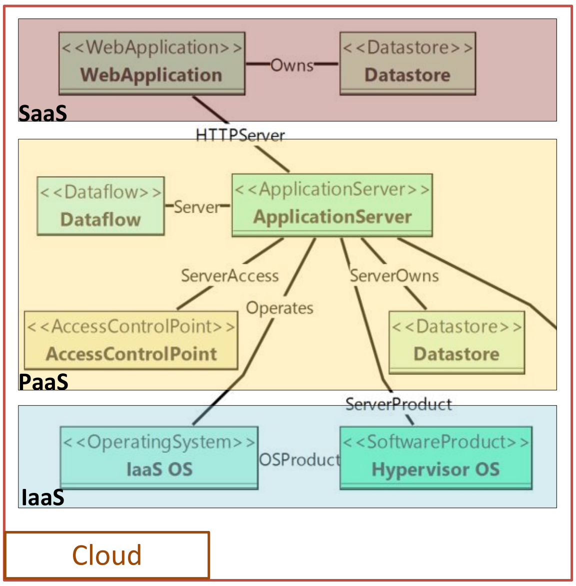

Fig. 2 – The model of the cloud computing delivery model stack in CySeMoL.

Since the security of public clouds is regulated by 3rd party service supplier and regulated by SLA, web application security controls, such as web application firewalls are disregarded in this model. Instead this issue is sorted by a newly proposed concept of SLA. The Service Level Agreement (SLA) is described by the relevant Service Level Objectives (SLOs) based on [22]. The SLOs in this case fall into two categories [26] – Quality of Service and Quality of Protection that describes means of how the information is protected.

3.7. Comparison of the Proposed Model with Existing Measures

Based on the model, a test security assessment for the model was performed with varying attack points. For the demonstration, a scenario where an attacker exploits the SQL injection to the web application has been chosen. This model provided an overall evaluation of security aspects, however, only the most probable were selected for representation. The acquired data is then compared to the statistical data provided by the Cloud Security Alliance [27]. The distribution of threat occurrence probability is presented in Table 2. The threat mapping to CySeMoL attack steps leaves T1, T3-T4, T8-T10 for the newly introduced SLA concept, while others are mapped directly to the matching attack steps. The comparison of the threat occurrence distribution is presented in Fig. 6.

Table 2

Threat occurrence probability based on [27]

Threat	Probability, %	Threat	Probability, %
T1. Abuse and Nefarious Use of Cloud Computing	7	T7. Unknown Risk Profile	6
T2. Insecure Interfaces and APIs	29	T8. Hardware Failure	10
T3. Malicious Insiders	2	T9. Natural Disasters	2
T4. Shared Technology Issues	3	T10. Closure of Cloud Service	2
T5. Data Loss or Leakage	25	T11. Cloud-related Malware	3
T6. Account or Service Hijacking	2	T12. Inadequate Infrastructure Design and Planning	9

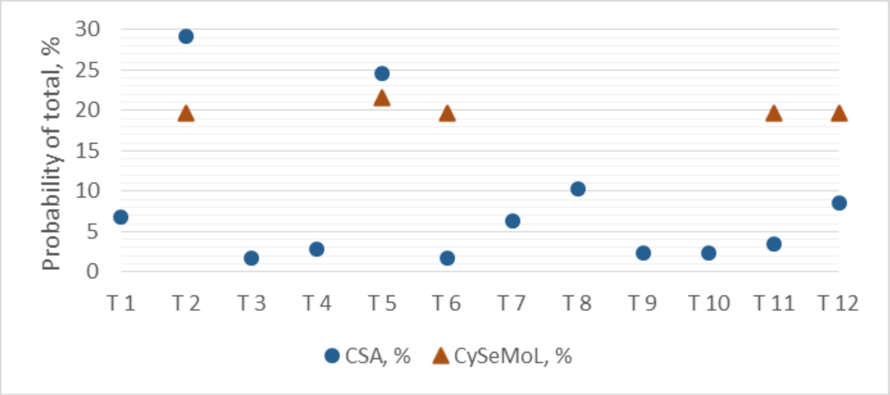

Fig. 3 – The comparison of the threat occurrence distribution.

Figure 6 introduces the most vulnerable aspects of SQL injection to the web application. Insecure interfaces and APIs is the most common issue. However, the implementation of SLA would minimize the threat frequency, as cloud vendor would take more responsibility for the security controls on vendor side of infrastructure. As visible from Fig. 6, current CySeMoL version covers 5 of 12 critical threats [27] of cloud computing information security, while the rest of the threats would be covered by regulatory contractual conditions [22].

4. CONCLUSIONS

Overview of previous research in the field has shown that although cloud computing is an emerging area of information sciences, the tools and methods for cloud computing information security assessment is still a relatively new subject, requiring more attention. Enterprise architecture analysis enables complex information security assessment, covering a broad range of issues found in such an architecture. An extension is required to assess information security of cloud computing in CySeMoL. A new meta-concept introducing contractual relations – the Service Level Agreement as a control measure extending the capabilities of CySeMoL is introduced in this paper.

REFERENCES

1. M. J. KAVIS, *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, IaaS)*, Hoboken, John Wiley & Sons, 2014, p. 351.
2. T. SOMMESTAD, M. EKSTEDT, H. HOLM, *The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise System Architectures*, Systems Journal, vol. 7, pp. 363-373, 2013.
3. S. FRIEDENTHAL, A. MOORE, R. STEINER, A Practical Guide to SysML, Waltham, Elsevier, 2014.
4. M. CHINOSI, A. TROMBETTA, *BPMN: An introduction to the standard*, Computer Standards & Interfaces, **34**, pp. 124-134, 2012.
5. L. LEMAIRE , J. LAPON, *A SysML Extension for Security Analysis of Industrial Control Systems,* 2nd International Symposium for ICS & SCADA Cyber Security Research 2014 (ICS-CSR 2014), St Pölten, 2014.
6. F. MACHIDA, E. ANDRADE, D. S. KIM, K. S. TRIVEDI, *Candy: Component-based Availability Modeling Framework for Cloud Service Management Using SysML*, The 30th IEEE Symposium on Reliable Distributed Systems (SRDS 2011), Madrid, 2011.
7. H. HOLM, M. EKSTEDT, T. SOMMESTAD, M. KORMAN, *A Manual for the Cyber Security Modeling Language*, Department of Industrial Information and Control Systems, Royal Institute of Technology, Stockholm, 2013.
8. K. BECKERS, M. HEISEL, B. SOLHAUG, K. STØLEN, *ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System*, in Engineering Secure Future Internet Services and Systems, Heidelberg, Springer, 2014, pp. 315-344.
9. X. OU, S. GOVINDAVAJHALA, A. W. APPEL, *MulVAL: A Logic-based Network Security Analyzer*, 14th USENIX Security Symposium, Baltimore, 2005.
10. M. L. ARTZ, *NetSPA: A Network Security Planning Architecture*, Massachussetts Institute of Technology, Cambridge, 2002.
11. E. C. ANDRADE, M. ALVES, R. MATOS, B. SILVA, P. MACIEL, *OpenMADS: An Open Source Tool for Modeling and Analysis of Distributed Systems*, in Computer Safety, Reliability, and Security. Lecture Notes in Computer Science Volume 8153, Heidelberg, Springer, 2013, pp. 277-284.
12. INTEL IT CENTER, *Cloud Security. Seven Steps for Building Security in the Cloud from Ground Up. Planning Guide*, Intel IT Center, 2012.
13. C. C. WEBER, *Assessing Security Risk in Legacy Systems*, Build Security In, 2013.
14. CONTEXT INFORMATION SECURITY, LTD., *Assessing Cloud Node Security*, Context Information Security, Ltd., London, 2011.
15. D. CATTEDDU, G. HOGBEN, *Cloud Computing: Benefits, Risks and Recommendations for Information Security*, European Network and Information Security Agency, Heraklion, 2009.
16. J. SZEFER, E. KELLER, R. B. LEE, J. REXFORD, *Eliminating the Hypervisor Attack Surface for a More Secure Cloud*, Conference on Computer and Communications Security, Chicago, 2011.
17. Y. ZHANG, A. JUELS, A. OPREA, M. K. REITER, *HomeAlone: Co-residency Detection in the Cloud via Side-Channel Analysis*, IEEE Symposium on Security and Privacy (SP), Berkeley, 2011.
18. C. WANG, Q. WANG, K. REN, W. LOU, *Ensuring Data Storage Security in Cloud Computing*, IEEE Infocom, San Diego, 2010.
19. M. HOWARD, J. PINCUS, J. M. WING, *Measuring Relative Attack Surfaces*, Carnegie-Mellon University, Pittsburgh, 2003.
20. N. GRUSCHKA, M. JENSEN, *Attack Surfaces: A Taxonomy for Attacks on Cloud Services*, IEEE 3rd International Conference on Cloud Computing, 2010.
21. International Organization for Standardization, *Information technology Cloud computing: Service level agreement (SLA) framework and Technology Part 1: Overview and concepts*, ISO/IEC CD 19086-1, 2015.
22. European Commission, *Cloud Service Level Agreement Standardisation Guidelines*, The Cloud Select Industry Group. Subgroup on Service Level Agreements, Brussels, 2014.
23. D. C. MARINESCU, *Cloud Computing – Theory and Practice*, Elsevier, Amsterdam, 2013.
24. D. KYRIAZIS, *Cloud Computing Service Level Agreements. Exploitation of Research Results*, European Commission Directorate General Communications Networks, Content And Technology Unit E2 – Software And Services, Cloud, Brussels, 2013.
25. F. LIU, J. TONG, J. MAO, R. BOHN, J. MESSINA, L. BADGER, D. LEAF, *NIST SP 500-292. NIST Cloud Computing Reference Architecture*, National Institute of Standards and Technology, Gaithersburg, 2011.
26. D. GOLLMANN, F. MASSACCI, A. YAUTSIUKHIN, *Quality of Protection: Security Measurements and Metrics*, New York, Springer, 2006.
27. CLOUD VULNERABILITIES WORKING GROUP, *Cloud Computing Vulnerability Incidents: A Statistical Overview*, Cloud Security Alliance, 2013.

Received July 7, 2015